

# COMPOSITIONAL INVERSES, COMPLETE MAPPINGS, ORTHOGONAL LATIN SQUARES AND BENT FUNCTIONS

ALEKSANDR TUXANIDY AND QIANG WANG

**ABSTRACT.** We study compositional inverses of permutation polynomials, complete mappings, mutually orthogonal Latin squares, and bent vectorial functions. Recently it was obtained in [33] the compositional inverses of linearized permutation binomials over finite fields. It was also noted in [29] that computing inverses of bijections of subspaces have applications in determining the compositional inverses of certain permutation classes related to linearized polynomials. In this paper we obtain compositional inverses of a class of linearized binomials permuting the kernel of the trace map. As an application of this result, we give the compositional inverse of a class of complete mappings. This complete mapping class improves upon a recent construction given in [34]. We also construct recursively a class of complete mappings involving multi-trace functions. Finally we use these complete mappings to derive a set of mutually orthogonal Latin squares, and to construct a class of  $p$ -ary bent vectorial functions from the Maiorana-McFarland class.

## 1. INTRODUCTION

Let  $q = p^m$  be the power of a prime number  $p$ , let  $\mathbb{F}_q$  be a finite field with  $q$  elements, and let  $\mathbb{F}_q[x]$  be the ring of polynomials over  $\mathbb{F}_q$ . We call a polynomial  $f \in \mathbb{F}_q[x]$  a *permutation polynomial* (PP) over  $\mathbb{F}_q$  if it induces a permutation of  $\mathbb{F}_q$  under evaluation. We denote the *composition* of two polynomials  $f, g$  by  $(f \circ g)(x) := f(g(x))$ . It is clear that permutation polynomials over  $\mathbb{F}_q$  form a group under composition and subsequent reduction modulo  $x^q - x$  that is isomorphic to the symmetric group on  $q$  letters. Thus for any permutation polynomial  $f \in \mathbb{F}_q[x]$  there exists a unique  $f^{-1} \in \mathbb{F}_q[x]$  such that  $f(f^{-1}(x)) \equiv f^{-1}(f(x)) \equiv x \pmod{x^q - x}$ . We call  $f^{-1}$  the *compositional inverse* of  $f$  over  $\mathbb{F}_q$ .

The construction of permutation polynomials over finite fields is an old and difficult subject that continues to attract interest due to their applications in cryptography [22, 26], coding theory [9, 16], and combinatorics [10]. See also [1, 2, 3, 6, 8, 11, 12, 13, 14, 19, 20, 32, 39, 40, 41, 42], and the references therein for some recent work in the area. However, the problem of determining the compositional inverse of a permutation polynomial seems to be an even more complicated problem. In fact, there are very few known permutation polynomials whose explicit compositional inverses have been obtained [7, 29, 33, 37], and the resulting expressions are usually of a complicated nature except for the classes of the permutation linear polynomials, monomials, Dickson polynomials. In addition, see

---

*Date:* September 24, 2014.

*Key words and phrases.* Permutation polynomial, complete mapping, compositional inverse, linearized polynomial, Dickson matrix, trace, quasigroup, mutually orthogonal Latin square,  $p$ -ary bent vectorial function, Maiorana-McFarland class, finite fields.

PP (permutation polynomial); CPP (complete permutation polynomials or complete mappings); OLS (orthogonal Latin squares); MOLS (mutually orthogonal Latin squares).

The research of Aleksandr Tuxanidy and Qiang Wang is partially supported by OGS and NSERC, respectively, of Canada.

[21, 30] for the characterization of the inverse of permutations of  $\mathbb{F}_q$  with form  $x^r f(x^s)$  where  $s \mid (q-1)$ .

Of particular interest in the study of permutations of finite fields are the linearized polynomials. Polynomials with form  $L(x) := \sum_{i=0}^{n-1} a_i x^{q^i}$  are called *linearized polynomials* or  *$q$ -polynomials*, which are  $\mathbb{F}_q$ -linear maps when seen as operators of  $\mathbb{F}_{q^n}$ . Note that  $L$  is a permutation polynomial over  $\mathbb{F}_{q^n}$  if and only if its associate *Dickson matrix* given by

$$(1) \quad D_L = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix}$$

is non-singular [17]. We denote by  $\mathcal{L}_n(\mathbb{F}_{q^n})$  the set of all  $q$ -polynomials over  $\mathbb{F}_{q^n}$ . Recently Wu and Liu obtained in [36] an expression for the compositional inverse of  $L$  in terms of cofactors of  $D_L$ . Then using this result Wu computed in [33] the compositional inverses, in explicit form, of arbitrary linearized permutation binomials over finite fields.

More recently, Tuxanidy and Wang showed in [29] that the problem of computing the compositional inverses of certain classes of permutations is equivalent to obtaining the inverses of two other polynomials bijecting subspaces of the finite field, where one of these two is a linearized polynomial inducing a bijection between kernels of other linearized polynomials. For this they showed in Theorem 2.5 of [29] how to obtain linearized polynomials inducing the inverse map over subspaces on which a linearized polynomial induces a bijection. This in fact amounts to solving a system of linear equations. Thus, in particular, it is of interest to obtain explicit compositional inverses of linearized permutations of subspaces.

Denote by  $T_{q^n|q} : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_q$  the (linearized) *trace map* given by

$$T_{q^n|q}(x) = \sum_{i=0}^{n-1} x^{q^i}.$$

When it will not cause confusion, we abbreviate this with  $T$ . In Section 2 of this paper we determine a class of linearized binomials permuting the kernel of the trace map and proceed to obtain its inverses on the kernel. See Theorem 2.4 for more details.

*Complete permutation polynomials* (CPP) over  $\mathbb{F}_q$ , also called *complete mappings*, are permutation polynomials  $f \in \mathbb{F}_q[x]$  such that  $f(x) + x$  is also a permutation polynomial over  $\mathbb{F}_q$ . CPPs have recently become a strong source of interest due to their connection to combinatorial objects such as orthogonal Latin squares [24, 25], and due to their applications in cryptography; in particular, in the construction of bent functions [18, 23, 25, 27]. See also [28, 34, 35, 38] and the references therein for some recent work in the area. In Section 3 we study complete mappings and give an improvement (Theorem 3.4) to Theorem 3.7 of [34] by Wu-Lin. This result generalized some earlier corresponding ones found in [15, 25, 35, 38]. We also give a recursive construction of complete mappings involving multi-trace functions; see Corollary 3.6.

As an application of Theorem 2.4 where we obtained the compositional inverses of linearized binomials permuting the kernel of the trace, we derive in Section 4 the compositional inverse of the class of complete permutation polynomials in Theorem 3.4 generalizing some of the classes recently studied in [15, 25, 34, 35, 38]. Note that since inverses of complete mappings are also complete mappings, Theorem 4.2 and Corollary 4.3 imply the construction of a new, if rather complicated, class of complete permutation polynomials.

In Section 5 we use the new class to construct a set of mutually orthogonal Latin squares. Finally in Section 6 we derive a class of  $p$ -ary bent vectorial functions from the Maiorana-McFarland class by the means of our complete mapping.

Before we move on to the following sections let us fix the following notations and definitions. If we view  $f \in \mathbb{F}_q[x]$  as a map of  $\mathbb{F}_q$  and we are given a subset  $V$  of  $\mathbb{F}_q$ , we mean by  $f|_V$  the map obtained by restricting  $f$  to  $V$ , and  $f|_V^{-1}$  denotes the inverse map of  $f|_V$ . When the context is clear we may however denote by  $f|_V^{-1}$  a polynomial in  $\mathbb{F}_q[x]$  inducing the inverse map of  $f|_V$ . When a polynomial  $f$  is viewed as a mapping  $\mathbb{F}_q \rightarrow \mathbb{F}_q$ , we denote by  $1/f$  the polynomial  $f^{q-2}$ . Similarly if  $x$  is viewed as a point of  $\mathbb{F}_q$ , we denote  $1/f(x) := f(x)^{q-2}$ . In this case we call  $f^{-1}(x)$  the *preimage* of  $x$  under  $f$ .

## 2. INVERSES OF LINEARIZED BINOMIALS PERMUTING KERNELS OF TRACES

In this section we study the compositional inverses of binomials permuting the kernel of the trace map. More precisely, given a positive integer  $r < n$ , consider the binomial  $L_{c,r}(x) := x^{p^r} - cx \in \mathbb{F}_{q^n}[x]$ , where  $c \in \mathbb{F}_q$ . Note that  $L_{c,r}(\ker(T_{q^n|q})) \subseteq \ker(T_{q^n|q})$ , where  $\ker(T_{q^n|q}) = \{\beta^q - \beta \mid \beta \in \mathbb{F}_{q^n}\}$  is the kernel of the additive map of  $T_{q^n|q}$  on  $\mathbb{F}_{q^n}$ . We would like to discover what are the necessary and sufficient conditions for  $L_{c,r}$  to be a permutation of  $\ker(T_{q^n|q})$ , and in such cases obtain a polynomial in  $\mathbb{F}_{q^n}[x]$  inducing the inverse map of  $L_{c,r}|_{\ker(T_{q^n|q})}$ . We only need to consider the case when  $L_{c,r}$  permutes  $\mathbb{F}_{q^n}$  and the case when  $L_{c,r}$  permutes  $\ker(T_{q^n|q})$  but not  $\mathbb{F}_{q^n}$ . The former case has already been tackled in [33] (see Theorem 2.1 here) and so we focus on the latter case. We give the result in Theorem 2.5 of Section 2.1. In Corollary 2.9 we show that under some restrictions of the characteristic,  $p$ , and the extension degree,  $n$ ,  $L_{c,r}$  permutes  $\ker(T_{q^n|q})$  for each  $c \in \mathbb{F}_q$ . Then in Section 2.2 we explain the method used to obtain the result.

**2.1. Statement and proof of result.** The following result due to Wu gives the compositional inverses of linearized permutation binomials  $x^{q^r} - cx$  where  $c$  lies in the extension  $\mathbb{F}_{q^n}$ . In the case when  $c$  lies in  $\mathbb{F}_q$ , the binomial is a permutation of  $\ker(T_{q^n|q})$  and thus its inverse map over the kernel is clearly the restriction of the inverse over  $\mathbb{F}_{q^n}$  to  $\ker(T_{q^n|q})$ . We state this in Corollary 2.2. This accounts for the case when the binomial permuting the kernel of the trace has full rank. Later in Theorem 2.4 and 2.5 we tackle the case when the linearized binomial permutes the kernel of the trace map but not  $\mathbb{F}_{q^n}$ . Denote by  $N_{q^n|q} : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_q$  the *norm* function given by  $N_{q^n|q}(x) = x^{(q^n-1)/(q-1)}$ .

**Theorem 2.1 (Theorem 2.1, [33]).** *Let  $c \in \mathbb{F}_{q^n}^*$  and let  $d := (n, r)$ . Then  $L_{c,r}(x) := x^{q^r} - cx \in \mathbb{F}_{q^n}[x]$  permutes  $\mathbb{F}_{q^n}$  if and only if  $N_{q^n|q^d}(c) \neq 1$ , in which case the compositional inverse of  $L_{c,r}$  over  $\mathbb{F}_{q^n}$  is given by*

$$L_{c,r}^{-1}(x) = \frac{N_{q^n|q^d}(c)}{1 - N_{q^n|q^d}(c)} \sum_{i=0}^{\frac{n}{d}-1} c^{-\frac{q^{(i+1)r}-1}{q^r-1}} x^{q^{ir}}.$$

**Corollary 2.2.** *Let  $q = p^m$  be a power of a prime number  $p$ , let  $n, r$ , be positive integers and denote  $d := (nm, r)$ . If  $c \in \mathbb{F}_q$  satisfies  $N_{q^n|p^d}(c) \neq 1$ , then  $L_{c,r}(x) := x^{p^r} - cx \in \mathbb{F}_{q^n}[x]$  permutes  $\ker(T_{q^n|q})$ , having a compositional inverse over  $\ker(T_{q^n|q})$  given by*

$$L_{c,r}^{-1}(x) = \frac{N_{q^n|p^d}(c)}{1 - N_{q^n|p^d}(c)} \sum_{i=0}^{\frac{nm}{d}-1} c^{-\frac{p^{(i+1)r}-1}{p^r-1}} x^{p^{ir}}.$$

*Proof.* Substituting  $q$  and  $n$  with  $p$  and  $nm$ , respectively, in Theorem 2.1, we obtain that  $L_{c,r}$  permutes  $\mathbb{F}_{q^n}$ . But since  $L_{c,r}(\ker(T_{q^n|q})) \subseteq \ker(T_{q^n|q}) \subseteq \mathbb{F}_{q^n}$ , it follows that  $L_{c,r}$  permutes

$\ker(T_{q^n|q})$ . It now suffices to pick  $L_{c,r}^{-1}$  as a compositional inverse of  $L_{c,r}$  over  $\ker(T_{q^n|q})$ , which is obtained from Theorem 2.1 through the aforementioned substitutions.  $\square$

We now focus on the case when the linearized binomial permutes the kernel of the trace map but does not permute  $\mathbb{F}_{q^n}$ . We need the following lemma.

**Lemma 2.3.** *Let  $n, r, s$ , be positive integers such that  $s \mid n$  and  $d := (n, r) = (s, r)$ . Then the following two identities hold.*

- (i)  $T_{q^n|q^s} = T_{q^{nr/d}|q^{sr/d}}|_{\mathbb{F}_{q^n}}$ ;
- (ii)  $N_{q^s|q^d} = N_{q^{sr/d}|q^r}|_{\mathbb{F}_{q^s}}$ .

*Proof.* (i) Since  $(n/d, r/d) = 1$  and  $n/s \mid n/d$  (implying  $(n/s, r/d) = 1$ ), we have  $\{k \pmod{n/s} \mid 0 \leq k \leq n/s - 1\} = \{kr/d \pmod{n/s} \mid 0 \leq k \leq n/s - 1\}$  from which it follows that  $\{ks \pmod{n} \mid 0 \leq k \leq n/s - 1\} = \{ksr/d \pmod{n} \mid 0 \leq k \leq n/s - 1\}$ . Hence, for any  $\alpha \in \mathbb{F}_{q^n}$ , we get

$$T_{q^n|q^s}(\alpha) := \sum_{k=0}^{\frac{n}{s}-1} \alpha^{q^{ks}} = \sum_{k=0}^{\frac{n}{s}-1} \alpha^{q^{ksr/d}} =: T_{q^{nr/d}|q^{sr/d}}(\alpha)$$

as required.

(ii) Since  $(s/d, r/d) = 1$ , we have  $\{k \pmod{s/d} \mid 0 \leq k \leq s/d - 1\} = \{kr/d \pmod{s/d} \mid 0 \leq k \leq s/d - 1\}$ , implying  $\{kd \pmod{s} \mid 0 \leq k \leq s/d - 1\} = \{kr \pmod{s} \mid 0 \leq k \leq s/d - 1\}$ . Thus, for any  $\beta \in \mathbb{F}_{q^s}$ , we obtain

$$N_{q^s|q^d}(\beta) := \beta^{\sum_{k=0}^{\frac{s}{d}-1} q^{kd}} = \beta^{\sum_{k=0}^{\frac{s}{d}-1} q^{kr}} =: N_{q^{sr/d}|q^r}(\beta).$$

$\square$

**Theorem 2.4.** *Let  $q = p^m$  be a power of a prime number  $p$ , let  $n, r, s$ , be positive integers such that  $s \mid n$  and  $d := (n, r) = (s, r)$ , and let  $c \in \mathbb{F}_{q^s}$  such that  $N_{q^s|q^d}(c) = 1$ . Then the binomial  $L_{c,r}(x) := x^{q^r} - cx \in \mathbb{F}_{q^n}[x]$  induces a permutation of  $\ker(T_{q^n|q^s})$  if and only if  $p \nmid n/s$ . In this case the compositional inverse of  $L_{c,r}$  over  $\ker(T_{q^n|q^s})$  is given by*

$$L_{c,r}|_{\ker(T_{q^n|q^s})}^{-1}(x) = \sum_{j=0}^{\frac{s}{d}-1} c^{-\frac{q^{(j+1)r}-1}{q^r-1}} \left( \left( \frac{n}{s} \right)^{-1} \sum_{k=1}^{\frac{n}{s}-1} kx^{q^{\frac{ksr}{d}}} \right)^{q^{jr}}.$$

*Proof.* Assume that  $L_{c,r}$  does not permute  $\mathbb{F}_{q^s}$ , i.e.,  $N_{q^s|q^d}(c) \neq 1$ . Now suppose on the contrary that  $p \mid n/s$ . Then for any  $k \in \mathbb{F}_{q^s}$ , we have  $T_{q^n|q^s}(k) = kn/s = 0$ ; hence  $\mathbb{F}_{q^s} \subseteq \ker(T_{q^n|q^s})$ . Then noting  $L_{c,r}(\mathbb{F}_{q^s}) \subseteq \mathbb{F}_{q^s}$ , we obtain that  $L_{c,r}$  permutes  $\mathbb{F}_{q^s}$ , a contradiction. Necessarily, if  $N_{q^s|q^d}(c) = 1$  and  $L_{c,r}$  permutes  $\ker(T_{q^n|q^s})$ , then  $p \nmid n/s$ . To show that these are also sufficient conditions for  $L_{c,r}$  to permute  $\ker(T_{q^n|q^s})$ , it suffices to prove that  $L_{c,r}|_{\ker(T_{q^n|q^s})}^{-1}$ , given above, induces the inverse of  $L_{c,r}|_{\ker(T_{q^n|q^s})}$ . First observe that  $N_{q^s|q^d}(c)^{-q^r} = N_{q^s|q^d}(c)$  since  $d \mid r$ . Moreover  $c^{(q^{sr/d}-1)/(q^r-1)} = N_{q^s|q^d}(c) = 1$  by Lemma 2.3. For the sake of brevity denote  $R(x) := (n/s)^{-1} \sum_{k=1}^{\frac{n}{s}-1} kx^{q^{ksr/d}}$ . Now, for all  $x \in \ker(T_{q^n|q^s})$ ,

we have

$$\begin{aligned}
L_{c,r} \left( L_{c,r} |_{\ker(T_{q^n|q^s})}^{-1}(x) \right) &= L_{c,r} |_{\ker(T_{q^n|q^s})}^{-1}(x)^{q^r} - c L_{c,r} |_{\ker(T_{q^n|q^s})}^{-1}(x) \\
&= \sum_{j=0}^{\frac{s}{d}-1} \left( c^{-q^r \left( \frac{q^{(j+1)r}-1}{q^r-1} \right)} R(x)^{q^{(j+1)r}} - c^{-\frac{q^{(j+1)r}-1}{q^r-1}+1} R(x)^{q^{jr}} \right) \\
&= \sum_{j=1}^{\frac{s}{d}} c^{-q^r \left( \frac{q^{jr}-1}{q^r-1} \right)} R(x)^{q^{jr}} - \sum_{j=0}^{\frac{s}{d}-1} c^{-q^r \left( \frac{q^{jr}-1}{q^r-1} \right)} R(x)^{q^{jr}} \\
&= c^{-q^r \left( \frac{\frac{s}{d}r-1}{q^r-1} \right)} R(x)^{q^{\frac{s}{d}r}} - R(x) \\
&= R(x)^{q^{\frac{s}{d}r}} - R(x) \\
&= \left( \frac{n}{s} \right)^{-1} \sum_{k=1}^{\frac{n}{s}-1} k \left( x^{q^{(k+1)\frac{sr}{d}}} - x^{q^{k\frac{sr}{d}}} \right) \\
&= \left( \frac{n}{s} \right)^{-1} \left( \sum_{k=1}^{\frac{n}{s}} (k-1) x^{q^{k\frac{sr}{d}}} - \sum_{k=0}^{\frac{n}{s}-1} k x^{q^{k\frac{sr}{d}}} \right) \\
&= \left( \frac{n}{s} \right)^{-1} \left( \left( \frac{n}{s} - 1 \right) x - \sum_{k=1}^{\frac{n}{s}-1} x^{q^{k\frac{sr}{d}}} \right) \\
&= x - \left( \frac{n}{s} \right)^{-1} T_{q^{nr/d}|q^{sr/d}}(x) \\
&= x - \left( \frac{n}{s} \right)^{-1} T_{q^n|q^s}(x) \\
&= x
\end{aligned}$$

as required.  $\square$

By the means of some substitutions we obtain the following equivalent result.

**Theorem 2.5.** *Let  $q = p^m$  be a power of a prime number  $p$ , let  $n, r$ , be positive integers such that  $d := (nm, r) = (m, r)$ , and let  $c \in \mathbb{F}_q$  such that  $N_{q|p^d}(c) = 1$ . Then  $L_{c,r}(x) := x^{p^r} - cx$  induces a permutation of  $\ker(T_{q^n|q})$  if and only if  $p \nmid n$ . In this case the compositional inverse of  $L_{c,r}$  over  $\ker(T_{q^n|q})$  is given by*

$$L_{c,r} |_{\ker(T_{q^n|q})}^{-1}(x) = \sum_{j=0}^{\frac{m}{d}-1} c^{-\frac{p^{(j+1)r}-1}{p^r-1}} \left( n^{-1} \sum_{k=1}^{n-1} k x^{p^{\frac{kmr}{d}}} \right)^{p^{jr}}.$$

*Proof.* The result follows from Theorem 2.4 if we substitute  $q, s, n$ , there with  $p, m, nm$ , respectively.  $\square$

**Remark 2.6.** *Theorem 2.4 and 2.5 are equivalent. Indeed, given  $x^{q^r} - cx \in \mathbb{F}_{q^n}[x]$  satisfying Theorem 2.4, i.e.,  $c \in \mathbb{F}_{q^s}$  with  $s \mid n$ ,  $(s, r) = (n, r)$  and  $q = p^m$ , we get  $x^{q^r} - cx = x^{p^{mr}} - cx \in \mathbb{F}_{q_1^{n/s}}[x]$  where  $c \in \mathbb{F}_{q_1}$  with  $q_1 := q^s = p^{ms}$ ,  $T_{q^n|q^s} = T_{q_1^{n/s}|q_1}$ , and  $(ms \cdot n/s, mr) = (mn, mr) = (ms, mr)$ , satisfying Theorem 2.5. Now the fact that Theorem 2.5 follows from Theorem 2.4 implies the equivalence of the two.*

**Corollary 2.7 (Lemma 3.4, [34]).** *Let  $q = p^m$  be a power of a prime number  $p$ , let  $n, r$ , be positive integers such that  $(n, r) = 1$ , and let  $c \in \mathbb{F}_q$ . Then  $x^{p^r} - cx$  permutes  $\ker(T_{q^n|q})$  if and only if  $c$  belongs to the any of the following two cases.*

- (i)  $N_{q|p^{(m,r)}}(c) = 1$  and  $p \nmid n$ ;
- (ii)  $N_{q^n|p^{(m,r)}}(c) \neq 1$ .

*Proof.* Using the fact that  $d := (nm, r) = (m, r)$  because  $(n, r) = 1$  by assumption, the result (i) follows from Theorem 2.5, while (ii) follows from Corollary 2.2.  $\square$

**Remark 2.8.** *By choosing, say  $n = 8$  and  $m = r = 2$ , it is easy to see that the hypotheses of Theorem 2.5 are in fact more general than those of Corollary 2.7.*

The following corollary shows that under some restrictions of  $p$  and  $n$ ,  $L_{c,r}$  permutes  $\ker(T_{q^n|q})$  for each  $c \in \mathbb{F}_q$ . Later on in Section 3 we will make use of this result in order to construct a class of complete mappings.

**Corollary 2.9.** *Let  $q = p^m$  be a power of a prime number  $p$ , let  $n, r$ , be positive integers such that  $d := (nm, r) = (m, r)$ ,  $p \nmid n$ , and  $(n, p^d - 1) = 1$ . Then  $L_{c,r}(x) := x^{p^r} - cx$  induces a permutation of  $\ker(T_{q^n|q})$  for each  $c \in \mathbb{F}_q$ .*

*Proof.* If  $N_{q|p^d}(c) = 1$ , then  $L_{c,r}$  permutes  $\ker(T_{q^n|q})$  by Theorem 2.5 (because  $p \nmid n$  additionally, by assumption). Now assume  $N_{q|p^d}(c) \neq 1$ . We claim that  $N_{q|p^d}(c)^n \neq 1$ ; equivalently, since  $N_{q^n|p^d}(c) = N_{q|p^d} \circ N_{q^n|q}(c) = N_{q|p^d}(c)^n \neq 1$ ,  $L_{c,r}$  permutes  $\mathbb{F}_{q^n}$  and hence  $\ker(T_{q^n|q})$  by Corollary 2.2. Clearly, if  $c = 0$ , then  $L_{c,r}$  permutes  $\ker(T_{q^n|q})$ . If  $c \neq 0$ , denote by  $t$  the multiplicative order of  $N_{q|p^d}(c) \in \mathbb{F}_{p^d}^*$ . It is clear that  $t \mid (p^d - 1)$ . On the contrary suppose that  $N_{q|p^d}(c)^n = 1$ . Then  $t \mid n$  as well. As a result,  $t \mid (n, p^d - 1) = 1$  giving  $t = 1$ , a contradiction to our assumption  $N_{q|p^d}(c) \neq 1$ . It follows that  $L_{c,r}$  permutes  $\ker(T_{q^n|q})$  for all  $c \in \mathbb{F}_q$ .  $\square$

**2.2. Method used to obtain the inverse in Theorem 2.4.** We know from Theorem 2.1 that  $L_{c,r}(x) = x^{q^r} - cx$  is a permutation polynomial over  $\mathbb{F}_{q^n}$  if and only if  $N_{q^n|q^d}(c) \neq 1$ , where  $d = (n, r)$ . In this case  $L_{c,r}$  must also permute  $\ker(T_{q^n|q^s})$  if  $c \in \mathbb{F}_q$  and thus we may take  $L_{c,r}^{-1}$  to be the compositional inverse over  $\ker(T_{q^n|q^s})$ , as done in Corollary 2.2. In this subsection we consider the case when  $L_{c,r}$  permutes  $\ker(T_{q^n|q^s})$  but does not permute  $\mathbb{F}_{q^n}$  (Theorem 2.4), and attempt to obtain a compositional inverse over  $\ker(T_{q^n|q^s})$ . Our method bears similarity to that employed in [33] where the compositional inverse of linearized binomials with full rank was obtained. It consists of modifying the initial problem into an easier one via substitutions of the parameters  $q, n$ , and in our case,  $s$  as well, and then computing the inverse over a convenient super space of  $\ker(T_{q^n|q^s})$ .

If we let  $q_1 := q^d$ , where  $d := (n, r) = (s, r)$ , then  $L_{c,r}(x)$  becomes  $x^{q_1^{r/d}} - cx \in \mathbb{F}_{q^n}[x] = \mathbb{F}_{q_1^{n/d}}[x]$  with  $c \in \mathbb{F}_{q^s} = \mathbb{F}_{q_1^{s/d}}$ ,  $T_{q^n|q^s} = T_{q_1^{n/d}|q_1^{s/d}}$ ,  $N_{q^n|q^d}(c) = N_{q_1^{n/d}|q_1^{s/d}}(c) = 1$ , and  $(n/d, r/d) = (s/d, r/d) = 1$ . Thus we first consider the case when  $(n, r) = (s, r) = 1$ . Now view  $L_{c,r}$  as a polynomial over the composite field  $\mathbb{F}_{q^{nr}}$  and observe that  $L_{c,r} \in \mathcal{L}_n(\mathbb{F}_{q^{nr}})$ , i.e.,  $L_{c,r}$  is a  $q^r$ -polynomial over  $\mathbb{F}_{q^{nr}}$ . From Lemma 2.3 we know that  $T_{q^{nr}|q^{sr}}|_{\mathbb{F}_{q^n}} = T_{q^n|q^s}$  and thus  $\ker(T_{q^n|q^s}) = \ker(T_{q^{nr}|q^{sr}}|_{\mathbb{F}_{q^n}}) \subseteq \ker(T_{q^{nr}|q^{sr}})$ . Moreover  $L_{c,r}(\ker(T_{q^{nr}|q^{sr}})) \subseteq \ker(T_{q^{nr}|q^{sr}})$ . It follows that if  $L_{c,r}$  permutes  $\ker(T_{q^{nr}|q^{sr}})$ , then the inverse map of  $L_{c,r}|_{\ker(T_{q^n|q^s})}$  can be obtained from the inverse of  $L_{c,r}|_{\ker(T_{q^{nr}|q^{sr}})}$  by restricting its domain to  $\mathbb{F}_{q^n}$ . We make use of the following theorem in order to obtain the inverse of  $L_{c,r}$  over  $\ker(T_{q^{nr}|q^{sr}})$ . Let  $v_{q,n} : \mathcal{L}_n(\mathbb{F}_{q^n}) \rightarrow \mathbb{F}_{q^n}^n$  denote the natural map defined by  $v_{q,n}(\sum_{i=0}^{n-1} a_i x^{q^i}) = (a_0 \ a_1 \ \dots \ a_{n-1})$  (for simplicity we write vectors horizontally). Recall that a linear operator  $L$  on  $\mathbb{F}_q$  is called *idempotent* if  $L \circ L(x) = L(x)$  for all  $x \in \mathbb{F}_q$ .

**Theorem 2.10 (Theorem 2.5, [29]).** *Let  $V, \bar{V}$ , be two equally sized  $\mathbb{F}_q$ -subspaces of  $\mathbb{F}_{q^n}$ , let  $\varphi \in \mathcal{L}_n(\mathbb{F}_{q^n})$  induce a bijection from  $V$  to  $\bar{V}$ , and let  $D_\varphi$  be the associate Dickson matrix of  $\varphi$ . Then  $L \in \mathcal{L}_n(\mathbb{F}_{q^n})$  induces the inverse map of  $\varphi|_V$  if and only if  $v_{q,n}(L(x))D_\varphi = v_{q,n}(x - K(x))$  for some  $K \in \mathcal{L}_n(\mathbb{F}_{q^n})$  inducing an idempotent endomorphism of  $\mathbb{F}_{q^n}$  with  $\ker(K) = V$ .*

**Remark 2.11.** *The original statement of Theorem 2.5 of [29] only gave necessary conditions for  $L$  to induce the inverse map of  $\varphi|_V$ . However it is trivial to show that these are also sufficient.*

Since  $\ker(T_{q^{nr}|q^{sr}})$  is an  $\mathbb{F}_{q^r}$ -subspace of  $\mathbb{F}_{q^{nr}}$ , and  $L_{c,r} \in \mathcal{L}_n(\mathbb{F}_{q^{nr}})$  is a  $q^r$ -polynomial over  $\mathbb{F}_{q^{nr}}$  inducing (by assumption) a permutation of  $\ker(T_{q^{nr}|q^{sr}})$ , Theorem 2.10 applies. Noting that  $(n/s)^{-1}T_{q^{nr}|q^{sr}} \in \mathcal{L}_n(\mathbb{F}_{q^{nr}})$  is idempotent on  $\mathbb{F}_{q^{nr}}$  having kernel  $\ker(T_{q^{nr}|q^{sr}})$ , we know from Theorem 2.10 that  $L_{c,r}$  permutes  $\ker(T_{q^{nr}|q^{sr}})$  (hence  $\ker(T_{q^n|q^s})$ ) if and only if there exists a solution  $\bar{d} = (d_0, \dots, d_{n-1})$  to the linear equation

$$\begin{aligned} \bar{d}D_{L_r} &= v_{q^r,n} \left( x - \left( \frac{n}{s} \right)^{-1} T_{q^{nr}|q^{sr}}(x) \right) \\ &= - \left( \frac{n}{s} \right)^{-1} \left( 1 - \frac{n}{s}, 0, 0, \dots, 0, 1, 0, 0, \dots, 0, 1, 0, 0, \dots \right), \end{aligned}$$

where the non-zero entries on the right hand side occur at indices (which start at 0 and end at  $n-1$ ) given by  $ks$  with  $0 \leq k < n/s$ , and

$$D_{L_{c,r}} = \begin{pmatrix} -c & 1 & 0 & 0 & \dots & 0 \\ 0 & -c^{q^r} & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & 0 & 0 & 0 & \dots & -c^{q^{(n-1)r}} \end{pmatrix}$$

is the associate Dickson matrix of  $L_{c,r} \in \mathcal{L}_n(\mathbb{F}_{q^{nr}})$ . If so, it follows that the polynomial  $\sum_{i=0}^{n-1} d_i x^{q^{ir}}$  induces the inverse map of  $L_{c,r}|_{\ker(T_{q^{nr}|q^{sr}})}$ , and hence of  $L_{c,r}|_{\ker(T_{q^n|q^s})}$ . Solving the linear equation we obtain a solution

$$d_{ks+j} = \left( \frac{n}{s} \right)^{-1} kc^{-\frac{q^{(j+1)r}-1}{q^r-1}},$$

where  $0 \leq j < s$  and  $0 \leq k < n/s$ . To see this, it suffices to show that  $\bar{d}$  satisfies the linear equation, i.e., that the  $(ks+j)$ -th entry,  $(\bar{d}D_{L_{c,r}})_{ks+j}$ , of the  $n$ -tuple  $\bar{d}D_{L_{c,r}}$ , satisfies

$$(\bar{d}D_{L_{c,r}})_{ks+j} = \begin{cases} 1 - \left( \frac{n}{s} \right)^{-1} & \text{if } j = k = 0; \\ - \left( \frac{n}{s} \right)^{-1} & \text{if } j = 0 \text{ and } k \geq 1; \\ 0 & \text{otherwise,} \end{cases}$$

where  $0 \leq j < s$  and  $0 \leq k < n/s$ . First recall that we have made the assumptions that  $N_{q^s|q}(c^{-1}) = 1$  ( $d = 1$  since  $d := (n, r) = (s, r) = 1$  by our assumption above) and  $p \nmid n/s$  of

Theorem 2.4. Then Lemma 2.3 gives  $N_{q^{sr}|q^r}(c^{-1}) = 1$ . We have

$$\begin{aligned}
(\bar{d}D_{L_{c,r}})_0 &= -d_0c + d_{n-1} = 0 + d_{\left(\frac{n}{s}-1\right)s+s-1} \\
&= \left(\frac{n}{s}\right)^{-1} \left(\frac{n}{s} - 1\right) N_{q^{sr}|q^r}(c^{-1}) \\
&= 1 - \left(\frac{n}{s}\right)^{-1}; \\
(\bar{d}D_{L_{c,r}})_{0 < k < n/s}^{ks} &= -d_{ks}c^{q^{ksr}} + d_{ks-1} = -d_{ks}c + d_{(k-1)s+s-1} \\
&= \left(\frac{n}{s}\right)^{-1} \left[ -kc^{-1}c + (k-1) N_{q^{sr}|q^r}(c^{-1}) \right] \\
&= -\left(\frac{n}{s}\right)^{-1}; \text{ and} \\
(\bar{d}D_{L_{c,r}})_{0 < j < s}^{ks+j} &= -d_{ks+j}c^{q^{(ks+j)r}} + d_{ks+j-1} \\
&= \left(\frac{n}{s}\right)^{-1} k \left[ -c^{-\frac{q^{(j+1)r}-1}{q^r-1}} c^{q^{jr}} + c^{-\frac{q^{jr}-1}{q^r-1}} \right] \\
&= \left(\frac{n}{s}\right)^{-1} k \left[ -c^{-\frac{q^{jr}-1}{q^r-1}} + c^{-\frac{q^{jr}-1}{q^r-1}} \right] \\
&= 0,
\end{aligned}$$

as required. As a result, if  $(n, r) = 1$ , then  $N_{q^s|q}(c) = 1$  and  $p \nmid n/s$  are sufficient conditions for  $L_{c,r}$  to permute  $\ker(T_{q^n|q^s})$  but not  $\mathbb{F}_{q^n}$ . In this case, one of the polynomials inducing the inverse map of  $L_{c,r}|_{\ker(T_{q^n|q^s})}$  is given by

$$\begin{aligned}
L_{c,r}|_{\ker(T_{q^n|q^s})}^{-1}(x) &= \left(\frac{n}{s}\right)^{-1} \sum_{j=0}^{s-1} \sum_{k=1}^{\frac{n}{s}-1} kc^{-\frac{q^{(j+1)r}-1}{q^r-1}} x^{q^{(ks+j)r}} \\
&= \sum_{j=0}^{s-1} c^{-\frac{q^{(j+1)r}-1}{q^r-1}} \left( \left(\frac{n}{s}\right)^{-1} \sum_{k=1}^{\frac{n}{s}-1} kx^{q^{ksr}} \right)^{q^{jr}}.
\end{aligned}$$

Now for the general case of  $1 \leq r \leq n-1$  and  $d = (n, r) = (s, r)$ , substitute  $q, n, r, s$ , with  $q^d, n/d, r/d, s/d$ , respectively, in the expression above for  $L_{c,r}|_{\ker(T_{q^n|q^s})}^{-1}$ , to obtain the result in Theorem 2.4.

### 3. IMPROVEMENT OF A CLASS OF COMPLETE PERMUTATION POLYNOMIALS

In [34] Wu and Lin gave the following class of complete permutation polynomials which generalized some of the classes previously studied in [15, 25, 35, 38].

**Theorem 3.1 (Theorem 3.7, [34]).** *Let  $q = p^m$  be a prime power. Let  $G \in \mathbb{F}_q[x]$ , let  $r$  be a positive integer with  $(r, n) = 1$ , and assume  $p \nmid n$  and  $(n, p^{(m,r)} - 1) = 1$ . Then the polynomial*

$$x \left( G(T_{q^n|q}(x)) + aT_{q^n|q}(x)^{p^r-1} - ax^{p^r-1} \right)$$

*is a complete permutation polynomial over  $\mathbb{F}_{q^n}$  for each  $a \in \mathbb{F}_q^*$  if and only if  $xG(x)$  is a complete permutation polynomial over  $\mathbb{F}_q$ .*

In this section we improve upon this result by replacing the requirement that  $(n, r) = 1$  with the more general one of  $(m, r) = (mn, r)$ . See Theorem 3.4 below yielding Corollary 3.5. Finally in Corollary 3.6 we give a recursive construction of complete mappings involving multi-trace functions. In Section 5 we will use this construction to generate sets



of mutually orthogonal Latin squares, and in Section 6 the class will be of use in deriving a class of vectorial bent functions. First we need the following lemma due to Coulter-Henderson-Matthews, a consequence of the AGW Criterion given in Lemma 1.2 of [2].

**Lemma 3.2 (Theorem 3, [8]).** *Let  $q = p^m$  be a prime power, let  $g \in \mathbb{F}_q[x]$ , let  $H \in \mathbb{F}_q[x]$  be a  $p$ -polynomial, and let  $f(x) = H(x) + xg(T(x))$ . Then  $f(x)$  is a permutation polynomial over  $\mathbb{F}_{q^n}$  if and only if the following two conditions hold.*

- (i)  $\varphi_y(x) := H(x) + xg(y)$  induces a permutation of  $\ker(T) = \{\beta^q - \beta \mid \beta \in \mathbb{F}_{q^n}\}$  for each  $y \in \mathbb{F}_q$ .
- (ii)  $\bar{f}(x) := H(x) + xg(x)$  induces a permutation of  $\mathbb{F}_q$ .

The following consequence is straightforward.

**Corollary 3.3.** *Let  $q = p^m$  be a prime power and let  $g \in \mathbb{F}_q[x]$ . Then  $xg(T(x))$  is a permutation of  $\mathbb{F}_{q^n}$  if and only if  $xg(x)$  is a permutation of  $\mathbb{F}_q$  and  $g(0) \neq 0$ .*

The following represents an improvement to Theorem 3.7 in [34], replacing the hypothesis of  $(n, r) = 1$  there with the more general one of  $(mn, r) = (m, r)$ .

**Theorem 3.4.** *Let  $q = p^m$  be a power of a prime number  $p$ , let  $G \in \mathbb{F}_q[x]$ , and let  $n, r$ , be positive integers such that  $d := (m, r) = (mn, r)$ ,  $p \nmid n$  and  $(n, p^{(m,r)} - 1) = 1$ . Then*

$$f(x) = ax^{p^r} + x(G(T_{q^n|q}(x)) - aT_{q^n|q}(x)^{p^r-1})$$

*is a complete permutation polynomial over  $\mathbb{F}_{q^n}$  for each  $a \in \mathbb{F}_q^*$  if and only if  $xG(x)$  is a complete permutation polynomial over  $\mathbb{F}_q$ .*

*Proof.* Note that both  $f(x)$  and  $f(x) + x$  are instances of Lemma 3.2. It follows that  $f$  is a complete permutation polynomial over  $\mathbb{F}_{q^n}$  if and only if  $\varphi_y(x) := ax^{p^r} + x(G(y) - ay^{p^r-1}) = a[x^{p^r} + x(G(y) - ay^{p^r-1})/a]$  is a complete permutation polynomial over  $\ker(T_{q^n|q})$ , and  $\bar{f}(x) := ax^{p^r} + x(G(x) - ax^{p^r-1}) = xG(x)$  is a complete permutation polynomial over  $\mathbb{F}_q$ . The former holds for each  $a \in \mathbb{F}_q^*$  by Corollary 2.9, whereas the latter implies the result.  $\square$

Theorem 3.4 generalizes [34, Theorem 3.7], [15, Theorem 3], [25, Theorem 4.1], [35, Theorem 2.1], and [38, Theorem 6]. Letting  $G = b \in \mathbb{F}_q \setminus \{-1, 0\}$  be arbitrary in Theorem 3.4, the following corollary is straightforward.

**Corollary 3.5.** *Let  $q = p^m$  be a power of a prime number  $p$ , and let  $n, r$ , be positive integers such that  $d := (m, r) = (mn, r)$ ,  $p \nmid n$  and  $(n, p^{(m,r)} - 1) = 1$ . Then*

$$f(x) = a(x^{p^r} - xT_{q^n|q}(x)^{p^r-1}) + bx$$

*is a complete permutation polynomial over  $\mathbb{F}_{q^n}$  for each  $a \in \mathbb{F}_q$  and each  $b \in \mathbb{F}_q \setminus \{-1, 0\}$ .*

Finally we give a recursive construction of CPPs involving multi-trace functions.

**Corollary 3.6.** *Let  $q = p^m$  be a power of a prime number  $p$ , let  $n, r$  and  $1 =: d_0 \mid d_1 \mid \dots \mid d_n := n$  be positive integers such that  $p \nmid n$ ,  $(n, p^{(m,r)} - 1) = 1$  and  $(d_i m, r) = (d_j m, r)$  for each  $0 \leq i, j \leq n$ . Let  $a_0, \dots, a_{n-1}$ , be such that for  $0 \leq k \leq n-1$ ,  $a_k \in \mathbb{F}_{q^{d_k}}$  and  $\sum_{l=0}^k a_l \neq 0$ . Let  $f_0 \in \mathbb{F}_q[x]$ . Then*

$$f(x) = x \left( \sum_{k=0}^{n-1} a_k (x^{p^r-1} - T_{q^n|q^{d_k}}(x)^{p^r-1}) + \frac{f_0(T_{q^n|q}(x))}{T_{q^n|q}(x)} \right)$$

*is a complete permutation polynomial over  $\mathbb{F}_{q^n}$  if and only if  $f_0$  is a complete permutation polynomial over  $\mathbb{F}_q$  satisfying  $f_0(0) = 0$ .*

*Proof.* For the sake of brevity denote  $T_j^k := T_{q^{d_k}|q^{d_j}}$  if  $j \leq k$ . For each  $0 \leq i \leq n-1$ , let  $c_i := \sum_{l=0}^i a_l \in \mathbb{F}_{q^{d_i}}^*$  and recursively define the polynomials

$$f_{i+1}(x) := x \left( c_i x^{p^r-1} - c_i T_i^{i+1}(x)^{p^r-1} + \frac{f_i(T_i^{i+1}(x))}{T_i^{i+1}(x)} \right) \in \mathbb{F}_{q^{d_{i+1}}}[x].$$

If we substitute  $G(x)$ ,  $m$ ,  $n$ ,  $q$ , in Theorem 3.4, with  $x^{q^{d_i-2}}f_i(x)$ ,  $d_i m$ ,  $d_{i+1}/d_i$ ,  $q^{d_i}$ , respectively, then each  $f_{i+1}$  satisfies the conditions of Theorem 3.4. Indeed, we have  $(\frac{d_{i+1}}{d_i} \cdot d_i m, r) = (d_{i+1}m, r) = (d_i m, r)$  by assumption;  $p \nmid d_{i+1}/d_i$  (because  $p \nmid n$ ) and  $(\frac{d_{i+1}}{d_i}, p^{(d_i m, r)} - 1) = (d_{i+1}/d_i, p^{(m, r)} - 1) = 1$  since  $(d_{i+1}/d_i) \mid n$  and  $(n, p^{(m, r)} - 1) = 1$  by assumption as well. Then it follows from Theorem 3.4 that  $f_{i+1}$  is a CPP over  $\mathbb{F}_{q^{d_i(d_{i+1}/d_i)}} = \mathbb{F}_{q^{d_{i+1}}}$  if and only if  $x^{q^{d_i-1}}f_i(x)$  is a CPP over  $\mathbb{F}_{q^{d_i}}$ . Note that

$$x^{q^{d_i-1}}f_i(x)|_{\mathbb{F}_{q^{d_i}}} = \begin{cases} f_i(x), & \text{if } i \geq 1 \text{ (since } f_i(0) = 0 \text{ for each } i \geq 1); \\ x^{q-1}f_0(x), & \text{if } i = 0. \end{cases}$$

Denote  $H(x) := x^{q-1}f_0(x)$ . We claim that  $f_1$  is a CPP over  $\mathbb{F}_{q^{d_1}}$  if and only if  $f_0$  is a CPP over  $\mathbb{F}_q$  satisfying  $f_0(0) = 0$ . Indeed, if  $f_0(0) = 0$ , then  $H|_{\mathbb{F}_q} = f_0$  implying that  $f_1$  is CPP over  $\mathbb{F}_{q^{d_1}}$  if and only if  $f_0$  is a CPP over  $\mathbb{F}_q$ . On the other hand, if  $f_0(0) \neq 0$ , write  $f_0(x) = A(x) + b$  for some  $A \in \mathbb{F}_q[x]$  such that  $A(0) = 0$  and some  $b \in \mathbb{F}_q^*$ . We need to show that  $H$  is not a CPP over  $\mathbb{F}_q$ . On the contrary, suppose that  $H$  is a CPP (and hence PP) over  $\mathbb{F}_q$ . Since  $H(0) = 0$ , it follows that  $H$  permutes  $\mathbb{F}_q^*$ . But  $H|_{\mathbb{F}_q^*} = f_0|_{\mathbb{F}_q^*}$ . Then  $f_0$  permutes  $\mathbb{F}_q^*$ . This in turn implies that  $A$  permutes  $\mathbb{F}_q^*$ . Hence  $-b \in A(\mathbb{F}_q^*)$  giving  $f_0(e) = 0$  for some  $e \in \mathbb{F}_q^*$ . But then  $H(e) = H(0) = 0$ , a contradiction. The claim follows. Now induction yields that for  $1 \leq i \leq n$ ,  $f_i$  is a CPP over  $\mathbb{F}_{q^{d_i}}$  if and only if  $f_0$  is a CPP over  $\mathbb{F}_q$  satisfying  $f_0(0) = 0$ . Next, assuming  $f_0(0) = 0$ , we claim that for  $0 \leq i \leq n$ ,

$$(2) \quad f_i(x) = x \left( \sum_{k=0}^{i-1} a_k (x^{p^r-1} - T_k^i(x)^{p^r-1}) + \frac{f_0(T_0^i(x))}{T_0^i(x)} \right).$$

Proceed by induction on  $0 \leq i \leq n$ . When  $i = 0$  the claim is clear. Assume (2) holds for some  $i < n$ . Then by the transitivity of the trace function, we get

$$\frac{f_i(T_i^{i+1}(x))}{T_i^{i+1}(x)} = \sum_{k=0}^{i-1} a_k (T_i^{i+1}(x)^{p^r-1} - T_k^{i+1}(x)^{p^r-1}) + \frac{f_0(T_0^{i+1}(x))}{T_0^{i+1}(x)}.$$

Thus, by the definition of  $f_{i+1}$ , we have

$$\begin{aligned}
f_{i+1}(x) &= x \left( c_i x^{p^r-1} - c_i T_i^{i+1}(x)^{p^r-1} \right. \\
&\quad \left. + \sum_{k=0}^{i-1} a_k (T_i^{i+1}(x)^{p^r-1} - T_k^{i+1}(x)^{p^r-1}) + \frac{f_0(T_0^{i+1}(x))}{T_0^{i+1}(x)} \right) \\
&= x \left( \sum_{k=0}^i a_k x^{p^r-1} - \sum_{k=0}^i a_k T_i^{i+1}(x)^{p^r-1} \right. \\
&\quad \left. + \sum_{k=0}^{i-1} a_k (T_i^{i+1}(x)^{p^r-1} - T_k^{i+1}(x)^{p^r-1}) + \frac{f_0(T_0^{i+1}(x))}{T_0^{i+1}(x)} \right) \\
&= x \left( \sum_{k=0}^i a_k x^{p^r-1} - \sum_{k=0}^i a_k T_k^{i+1}(x)^{p^r-1} + \frac{f_0(T_0^{i+1}(x))}{T_0^{i+1}(x)} \right) \\
&= x \left( \sum_{k=0}^i a_k \left( x^{p^r-1} - T_k^{i+1}(x)^{p^r-1} \right) + \frac{f_0(T_0^{i+1}(x))}{T_0^{i+1}(x)} \right),
\end{aligned}$$

satisfying the expression in (2). The claim follows. Now it only remains to notice that  $f = f_n$ .  $\square$

Corollary 3.6 generalizes [25, Corollary 4.4] and [35, Corollary 2.3].

#### 4. INVERSE OF THE COMPLETE MAPPING

In this section we obtain the compositional inverse of the complete mapping of Theorem 3.4. See Theorem 4.2 and Corollary 4.3 for this. To achieve this, we make use of the result in Section 2 of the compositional inverses of linearized binomials permuting the kernel of the trace map. Since inverses of complete mappings are also complete mappings, this signifies the construction of a new, albeit complicated, class of complete mappings.

We first introduce some notation. Let  $f_y \in \mathbb{F}_q[x]$  be a polynomial with parameter  $y \in \mathbb{F}_q$  and inducing an injective map on a subset  $V$  of  $\mathbb{F}_q$ . Let  $f_y|_V^{-1} \in \mathbb{F}_q[x]$  be the polynomial inducing the inverse map of  $f|_V$ . Then, for any  $g \in \mathbb{F}_q[x]$ , we mean by  $f_{g(x)}|_V^{-1}(x) \in \mathbb{F}_q[x]$  the polynomial obtained by substituting  $y$  with  $g(x) \in \mathbb{F}_q[x]$  in the expression for  $f_y|_V^{-1}(x)$ .

**Lemma 4.1 (Corollary 3.14, [29]).** *Using the same notations of Lemma 3.2 and assuming that  $f$  permutes  $\mathbb{F}_{q^n}$ , the following two results hold:*

(i) *If  $p \mid n$  or  $x \in \mathbb{F}_{q^n}$  is such that  $\varphi_{\bar{f}^{-1}(T(x))}$  permutes  $\mathbb{F}_q$ , then  $\varphi_{\bar{f}^{-1}(T(x))}$  permutes  $\mathbb{F}_{q^n}$ , and the preimage of  $x$  under  $f$  is given by*

$$f^{-1}(x) = \varphi_{\bar{f}^{-1}(T(x))}^{-1}(x),$$

where  $\bar{f}^{-1} := \bar{f}|_{\mathbb{F}_q}^{-1}$ .

(ii) *If  $p \nmid n$ , then the compositional inverse of  $f$  over  $\mathbb{F}_{q^n}$  is given by*

$$f^{-1}(x) = n^{-1} \bar{f}^{-1}(T(x)) + \varphi_{\bar{f}^{-1}(T(x))}|_{\ker(T)}^{-1}(x - n^{-1}T(x)).$$

Recall that  $1/f := f^{q-2}$  for a polynomial  $f$  if  $\text{im}(f) \subseteq \mathbb{F}_q$  when  $f$  is viewed as a mapping.

**Theorem 4.2.** Assume that the polynomial  $f$  of Theorem 3.4 is a permutation polynomial over  $\mathbb{F}_{q^n}$ . Then  $\bar{f}(x) := xG(x)$  is a permutation polynomial over  $\mathbb{F}_q$  and  $\varphi_y(x) := ax^{p^r} + x(G(y) - ay^{p^r-1})$  induces a permutation of  $\ker(T)$  for each  $y \in \mathbb{F}_q$ . Let  $\bar{f}^{-1} \in \mathbb{F}_q[x]$  denote the compositional inverse of  $\bar{f}$  over  $\mathbb{F}_q$  and define the polynomial

$$C(x) := \bar{f}^{-1}(T(x))^{p^r-1} - a^{-1}G(\bar{f}^{-1}(T(x))) \in \mathbb{F}_q[x].$$

Then the following three results hold:

(i) If  $x \in \mathbb{F}_{q^n}$  is such that  $C(x) = 0$ , then the preimage of  $x$  under  $f$  is given by

$$f^{-1}(x) = \left(\frac{x}{a}\right)^{\frac{q^n}{p^r}}.$$

(ii) Otherwise if  $x \in \mathbb{F}_{q^n}$  is such that  $N_{q|p^d}(C(x)) \neq 1$ , then  $N_{q|p^d}(C(x))^n \neq 1$ , and the preimage of  $x$  under  $f$  is given by

$$f^{-1}(x) = \frac{N_{q|p^d}(C(x))^n}{1 - N_{q|p^d}(C(x))^n} \sum_{i=0}^{\frac{nm}{d}-1} C(x)^{-\frac{p^{(i+1)r}-1}{p^r-1}} (a^{-1}x)^{p^{ir}}.$$

(iii) Otherwise the preimage of  $x \in \mathbb{F}_{q^n}$  under  $f$  is given by

$$f^{-1}(x) = n^{-1} \left( \bar{f}^{-1}(T(x)) + \sum_{j=0}^{\frac{m}{d}-1} C(x)^{-\frac{p^{(j+1)r}-1}{p^r-1}} \left( a^{-1} \sum_{k=1}^{n-1} kx^{p^{km}\frac{r}{d}} \right)^{p^{jr}} \right).$$

*Proof.* Write  $f(x) = ax^{p^r} - xg(T(x))$  where  $g(x) := ax^{p^r-1} - G(x)$ . As we have seen in the proof of Theorem 3.4, the fact that  $f$  is a PP over  $\mathbb{F}_{q^n}$  implies that  $\bar{f}(x) := xG(x)$  is a PP over  $\mathbb{F}_q$  and  $\varphi_y(x) := ax^{p^r} - xg(y) = a(x^{p^r} - xg(y)/a) = aL_{g(y)/a,r}(x)$  induces a permutation of  $\ker(T)$  for each  $y \in \mathbb{F}_q$ . Note that  $\varphi_y|_{\ker(T)}^{-1}(x) = L_{g(y)/a,r}|_{\ker(T)}^{-1}(a^{-1}x)$ , where  $L_{c,r}(x) := x^{p^r} - cx$  for  $c \in \mathbb{F}_q$ . Moreover  $C(x) = g(\bar{f}^{-1}(T(x)))/a$ .

(i): If  $x \in \mathbb{F}_{q^n}$  is such that  $C(x) = 0$ , then  $\varphi_{\bar{f}^{-1}(T(x))}(x) = aL_{C(x),r}(x) = ax^{p^r}$  permutes  $\mathbb{F}_{q^n}$ . Now Lemma 4.1 (i) gives

$$f^{-1}(x) = \varphi_{\bar{f}^{-1}(T(x))}^{-1}(x) = L_{g(y)/a,r}^{-1}(a^{-1}x) = \left(\frac{x}{a}\right)^{\frac{q^n}{p^r}}.$$

(ii) Otherwise if  $x \in \mathbb{F}_{q^n}$  is such that  $N_{q|p^d}(C(x)) \neq 1$ , then, by similar arguments to those in the proof of Corollary 2.9, we get

$$N_{q^n|p^d} \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right) = N_{q|p^d} \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)^n \neq 1.$$

Then by Corollary 2.2,  $L_{g(\bar{f}^{-1}(T(x)))/a,r}$ , and hence  $\varphi_{\bar{f}^{-1}(T(x))}$ , permute  $\mathbb{F}_{q^n}$ . Since  $\varphi_y(\mathbb{F}_q) \subseteq \mathbb{F}_q$  for each  $y \in \mathbb{F}_q$ , necessarily  $\varphi_{\bar{f}^{-1}(T(x))}$  permutes  $\mathbb{F}_q$ . Thus we can apply Lemma 4.1 (i) to obtain

$$f^{-1}(x) = \varphi_{\bar{f}^{-1}(T(x))}^{-1}(x) = L_{g(\bar{f}^{-1}(T(x)))/a,r}^{-1}(a^{-1}x).$$

Substituting  $c$  with  $g(\bar{f}^{-1}(T(x)))/a$  in Corollary 2.2, we get

$$f^{-1}(x) = \frac{N_{q^n|p^d} \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)}{1 - N_{q^n|p^d} \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)} \sum_{i=0}^{\frac{nm}{d}-1} \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)^{-\frac{p^{(i+1)r}-1}{p^r-1}} (a^{-1}x)^{p^{ir}}.$$

Now the result follows from the fact that  $N_{q^n|p^d}(y) = N_{q|p^d}(y)^n$  for any  $y \in \mathbb{F}_q$ .

(iii) Here we can use Theorem 2.5 to obtain the inverse of  $L_{g(\bar{f}^{-1}(T(x)))/a,r}|_{\ker(T)}$ . Since  $L_{g(\bar{f}^{-1}(T(x)))/a,r}$ , and hence  $\varphi_{\bar{f}^{-1}(T(x))}$ , do not permute  $\mathbb{F}_{q^n}$ , we apply Lemma 4.1 (ii) instead. This gives

$$\begin{aligned} f^{-1}(x) &= n^{-1} \bar{f}^{-1}(T(x)) + \varphi_{\bar{f}^{-1}(T(x))}|_{\ker(T)}^{-1} (x - n^{-1}T(x)) \\ &= n^{-1} \bar{f}^{-1}(T(x)) + L_{g(\bar{f}^{-1}(T(x)))/a,r}|_{\ker(T)}^{-1} (a^{-1} (x - n^{-1}T(x))). \end{aligned}$$

For the sake of brevity denote  $\bar{L}(z) := L_{g(\bar{f}^{-1}(T(x)))/a,r}|_{\ker(T)}^{-1}(z) \in \mathbb{F}_q[z]$ . Since  $\bar{L}$  is a  $p$ -polynomial, the above becomes

$$f^{-1}(x) = n^{-1} \bar{f}^{-1}(T(x)) + \bar{L}(a^{-1}x) - \bar{L}(a^{-1}n^{-1}T(x)).$$

By the definition of  $\bar{L}$  and by Theorem 2.5 with  $c = g(\bar{f}^{-1}(T(x)))/a$ , we get

$$\begin{aligned} \bar{L}(a^{-1}n^{-1}T(x)) &= \sum_{j=0}^{\frac{m}{d}-1} \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)^{-\frac{p^{(j+1)r}-1}{p^r-1}} \left( n^{-2} \sum_{k=1}^{n-1} k a^{-1}T(x) \right)^{p^{jr}} \\ &= \frac{n^{-1}(n-1)}{2} \sum_{j=0}^{\frac{m}{d}-1} \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)^{-\frac{p^{(j+1)r}-1}{p^r-1}} (a^{-1}T(x))^{p^{jr}}. \end{aligned}$$

Since  $\bar{f}(y) = yG(y) = ay^{p^r} - yg(y)$  for any  $y \in \mathbb{F}_q$ , we have  $y = a\bar{f}^{-1}(y)^{p^r} - \bar{f}^{-1}(y)g(\bar{f}^{-1}(y))$ . Then, if we substitute  $y$  with  $T(x)$ , the above becomes

$$\begin{aligned} \bar{L}(a^{-1}n^{-1}T(x)) &= \frac{n^{-1}(n-1)}{2} \sum_{j=0}^{\frac{m}{d}-1} \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)^{-\frac{p^{(j+1)r}-1}{p^r-1}} \\ &\quad \cdot \left( \bar{f}^{-1}(T(x))^{p^r} - \bar{f}^{-1}(T(x)) \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)^{p^{jr}} \\ &= \frac{n^{-1}(n-1)}{2} \sum_{j=0}^{\frac{m}{d}-1} \left( \bar{f}^{-1}(T(x))^{p^{(j+1)r}} \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)^{-\frac{p^{(j+1)r}-1}{p^r-1}} \right. \\ &\quad \left. - \bar{f}^{-1}(T(x))^{p^{jr}} \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)^{-\frac{p^{jr}-1}{p^r-1}} \right) \\ &= \frac{n^{-1}(n-1)}{2} \bar{f}^{-1}(T(x)) \left( \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)^{-\frac{p^{mr/d}-1}{p^r-1}} - 1 \right) \\ &= 0 \end{aligned}$$

because, by Lemma 2.3 (ii) and by assumption,

$$\left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)^{\frac{p^{mr/d}-1}{p^r-1}} = \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)^{\frac{p^m-1}{p^d-1}} = 1.$$

Thus

$$\begin{aligned} f^{-1}(x) &= n^{-1} \bar{f}^{-1}(T(x)) + L_{g(\bar{f}^{-1}(T(x)))/a, r} \big|_{\ker(T)}^{-1} (a^{-1}x) \\ &= n^{-1} \bar{f}^{-1}(T(x)) + \sum_{j=0}^{\frac{m}{d}-1} \left( \frac{g(\bar{f}^{-1}(T(x)))}{a} \right)^{-\frac{p^{(j+1)r}-1}{p^r-1}} \left( n^{-1} \sum_{k=1}^{n-1} k a^{-1} x^{p^{km} \frac{r}{d}} \right)^{p^{jr}}. \end{aligned}$$

The result follows.  $\square$

**Corollary 4.3.** *If the polynomial  $f$  in Theorem 3.4 is a permutation polynomial over  $\mathbb{F}_{q^n}$ , then its compositional inverse over  $\mathbb{F}_{q^n}$  is given by*

$$\begin{aligned} f^{-1}(x) &= (1 - C(x)^{q-1}) \left( \frac{x}{a} \right)^{\frac{q^n}{p^r}} \\ &\quad + C(x)^{q-1} (N_{q|p^d}(C(x)) - 1)^{p^d-1} \frac{N_{q|p^d}(C(x))^n}{1 - N_{q|p^d}(C(x))^n} \\ &\quad \cdot \sum_{i=0}^{\frac{mn}{d}-1} C(x)^{-\frac{p^{(i+1)r}-1}{p^r-1}} (a^{-1}x)^{p^{ir}} \\ &\quad + \left( 1 - (N_{q|p^d}(C(x)) - 1)^{p^d-1} \right) \\ &\quad \cdot n^{-1} \left( \bar{f}^{-1}(T(x)) + \sum_{j=0}^{\frac{m}{d}-1} C(x)^{-\frac{p^{(j+1)r}-1}{p^r-1}} \left( a^{-1} \sum_{k=1}^{n-1} k x^{p^{km} \frac{r}{d}} \right)^{p^{jr}} \right). \end{aligned}$$

*Proof.* We put the results of Theorem 4.2 together. Note that this is a step function where only one of the three terms is non-zero at a time. The first term of the expression is non-zero only when  $C(x) = 0$  corresponding to the result in (i), while the second term is non-zero only when  $C(x) \neq 0$  and  $N_{q|p^d}(C(x)) \neq 1$  corresponding to (ii). The third term is non-zero otherwise; this corresponds to the result in (iii). These are the only possibilities for  $C(x)$  and so we are done.  $\square$

Corollary 4.3 generalizes [29, Corollary 4.6] and [35, Theorem 3.5].

## 5. A CLASS OF MUTUALLY ORTHOGONAL LATIN SQUARES

In this section we construct a class of mutually orthogonal Latin squares by the means of the class of complete mappings in Theorem 3.4. We give the result in Theorem 5.3. Our class generalizes that of Theorem 5.5 in [25].

Let us recall some definitions. A *quasigroup operation*  $*$  on a set  $G$  is a binary operation such that the equations  $x * u = v$  and  $u * y = v$  have a unique solution  $x, y$  for every  $u, v \in G$ . We call  $(G, *)$  a *quasigroup* of order  $|G|$ . The multiplication table of a quasigroup is called a *Latin square*. A mapping  $Q : G \times G \rightarrow G$  defines a quasigroup if the binary operation  $u * v = Q(u, v)$  is a quasigroup operation on  $G$ . Two quasigroups  $(G, *_1), (G, *_2)$  are *orthogonal* if the system of equations  $(x *_1 y, x *_2 y) = (r, s)$  has a unique solution  $(x, y)$  for every  $(r, s) \in G \times G$ . In this case the multiplication tables of the two quasigroups are called *orthogonal Latin squares* (OLS). A set of Latin squares such that each pair is mutually orthogonal is called a set of *mutually orthogonal Latin squares* (MOLS).

We need the following Theorem 5.1 and Lemma 5.2 dealing with fields of arbitrary characteristic. Theorem 5.1 is due to Sade [24] and gives a method, known as the *diagonal method*, of constructing Latin squares by using complete mappings. The case when the

characteristic of the field is 2 was already considered in Theorem 5.1 and Lemma 5.2 of [25], although the proofs are essentially identical. We however add the proofs here for the convenience of the reader.

**Theorem 5.1 ([24]).** *Let  $P$  be a complete mapping over  $\mathbb{F}_q$ . Then the mapping  $Q : \mathbb{F}_q^2 \rightarrow \mathbb{F}_q$  given by*

$$Q(x, y) = P(x + y) + y$$

*defines a quasigroup that possesses at least one orthogonal mate, the group  $(\mathbb{F}_q, +)$ .*

*Proof.* Since  $P$  is a complete mapping, both  $Q(u, y)$  and  $Q(x, u)$  are permutations for each  $u \in \mathbb{F}_q$ . It follows that  $Q$  defines a quasigroup. Now  $(\mathbb{F}_q, Q)$  is orthogonal to  $(\mathbb{F}_q, +)$  if and only if the equation

$$(P(x + y) + y, x + y) = (r, s)$$

has a unique solution  $(x, y)$  for each  $(r, s) \in \mathbb{F}_q^2$ . This is equivalent to

$$(x, y) = (P(s) + s - r, r - P(s))$$

and so a unique solution exists (since  $P$  is a complete mapping).  $\square$

The following lemma determines when two quasigroups, constructed in the same fashion as that of Theorem 5.1, are orthogonal to each other.

**Lemma 5.2.** *Let  $P_1$  and  $P_2$  be complete mappings over  $\mathbb{F}_q$ . Then the quasigroups corresponding to*

$$Q_1(x, y) = P_1(x + y) + y$$

$$Q_2(x, y) = P_2(x + y) + y$$

*are orthogonal if and only if  $P_2 - P_1$  is a permutation over  $\mathbb{F}_q$ .*

*Proof.*  $(\mathbb{F}_q, Q_1)$  is orthogonal to  $(\mathbb{F}_q, Q_2)$  if and only if

$$P_1(x + y) + y = r$$

$$P_2(x + y) + y = s$$

has a unique solution  $(x, y)$  for each  $(r, s) \in \mathbb{F}_q^2$ . The system is equivalent to

$$x = P_1^{-1}(r - y) - y$$

$$x = P_2^{-1}(s - y) - y.$$

It follows that  $(\mathbb{F}_q, Q_1)$  is orthogonal to  $(\mathbb{F}_q, Q_2)$  if and only if

$$P_1^{-1}(r - y) = P_2^{-1}(s - y)$$

has a unique solution for each  $(r, s) \in \mathbb{F}_q^2$ . This equation is equivalent to

$$r = y + P_1 \circ P_2^{-1}(s - y)$$

and hence to

$$s - r = (s - y) - P_1 \circ P_2^{-1}(s - y)$$

which has a unique solution if and only if  $I - P_1 \circ P_2^{-1}$  is a permutation over  $\mathbb{F}_q$ . Since  $P_2$  is a permutation, the last occurs if and only if  $P_2 - P_1$  is a permutation.  $\square$

We are now ready to give the construction of a set of mutually orthogonal Latin squares.

**Theorem 5.3.** *Let  $q = p^m$  be a power of a prime number  $p$  and let  $n, r$ , be positive integers such that  $(m, r) = (mn, r)$ ,  $p \nmid n$  and  $(n, p^{(m,r)} - 1) = 1$ . Let  $\{b_i\}$  be a subset of  $\mathbb{F}_q$  and let  $G \in \mathbb{F}_q[x]$  such that each  $\bar{f}_i(x) := x(G(x) + b_i)$  is a complete permutation polynomial over  $\mathbb{F}_q$ . For each such  $b_i$ , let  $a_i \in \mathbb{F}_q^*$ . Then the quasigroups,  $(\mathbb{F}_{q^n}, Q_j)$ , where*

$$Q_0(x, y) = x + y, \quad Q_i(x, y) = P_i(x + y) + y$$

with

$$P_i(x) = x(a_i x^{p^r-1} - a_i T_{q^n|q}(x)^{p^r-1} + G(T_{q^n|q}(x)) + b_i), \quad i \geq 1,$$

form a set of  $1 + |\{b_i\}|$  mutually orthogonal Latin squares of order  $q^n$ .

*Proof.* By Theorem 3.4, each  $P_i$  is a CPP over  $\mathbb{F}_{q^n}$  since each  $\bar{f}_i$  is a CPP over  $\mathbb{F}_q$  by assumption. Moreover, if  $i \neq j$ ,

$$(P_j - P_i)(x) = x \left[ (a_j - a_i) x^{p^r-1} - (a_j - a_i) T_{q^n|q}(x)^{p^r-1} + (b_j - b_i) \right]$$

is a permutation over  $\mathbb{F}_{q^n}$  by Corollary 3.5 (since  $b_j \neq b_i$ ). Now Lemma 5.2 and Theorem 5.1 imply the result.  $\square$

Theorem 5.3 generalizes [25, Theorem 5.5].

## 6. A $p$ -ARY BENT VECTORIAL FUNCTION FROM THE MAIORANA-MCFARLAND CLASS

As another application of the permutation class obtained in Theorem 3.4, in this section we construct a class of  $p$ -ary bent vectorial functions by the means of the Maiorana-McFarland class. Our result, given in Theorem 6.2, generalizes that of Theorem 5.9 in [25].

For a prime  $p$ , let  $\xi_p = e^{2\pi\sqrt{-1}/p}$ . The Walsh transform of a function  $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$  is the complex-valued function  $\hat{f}$  defined by

$$\hat{f}(b) = \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{f(x) + T_{p^n|p}(bx)}.$$

The function  $f$  is called a  $p$ -ary bent function if  $|\hat{f}(b)| = \sqrt{p^n}$  for all  $b \in \mathbb{F}_{p^n}$  (see for example [5]). Bent functions have the minimum correlation to the class of affine functions (or maximum *non-linearity* possible), an important concept in cryptography [23]. The construction of bent functions have been a focus of attention in several works. See for instance [5, 18, 23, 25, 27]. It was noted by Nyberg in [23] that complete mappings are useful in the construction of bent functions.

In general, a  $(n, m)$ -vectorial function  $F = (f_0, f_1, \dots, f_{m-1}) : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p^m$  is called  $(n, m)$ -bent if any non-zero linear combination of its components is a bent function. An amply studied class of bent functions in the literature is the Maiorana-McFarland class (see the aforementioned citations). These are the functions  $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$  with form

$$f(x, y) = T_{p^n|p}(x\pi(y) + g(y))$$

where  $\pi, g$ , are functions on  $\mathbb{F}_{p^n}$ . The condition that  $\pi$  is a permutation of  $\mathbb{F}_{p^n}$  is both necessary and sufficient for  $f$  to be bent. But in general we have the following:

**Lemma 6.1** ([23]). *The function  $F = (f_0, f_1, \dots, f_{m-1}) : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p^m$ , where each of the components  $f_i$  is a Maiorana-McFarland function*

$$f_i(x, y) = T_{p^n|p}(x\pi_i(y) + g_i(y)),$$

*is a  $(2n, m)$ -bent function if every non-zero linear combination over  $\mathbb{F}_p$  of the functions  $\pi_i$ , where  $i \in \{0, 1, \dots, m-1\}$ , is a permutation of  $\mathbb{F}_{p^n}$ .*



The following application of the complete mapping of Theorem 3.4 gives a new class of  $p$ -ary bent vectorial functions through the means of the Maiorana-McFarland class.

**Theorem 6.2.** *Let  $q = p^m$  be a power of a prime number  $p$  and let  $n, r$ , be positive integers such that  $(m, r) = (mn, r)$ ,  $p \nmid n$  and  $(n, p^{(m,r)} - 1) = 1$ . Let  $S$  be a subspace of  $\mathbb{F}_q$  over  $\mathbb{F}_p$  of dimension  $k \leq m$  and with some basis  $\{\alpha, \alpha^p, \dots, \alpha^{p^{k-1}}\}$ . Let  $G \in \mathbb{F}_q[x]$  be such that  $G(0) \notin S \setminus \{0\}$  and  $\bar{f}(x) := x(G(x) + b)$  is a permutation polynomial over  $\mathbb{F}_q$  for each  $b \in S \setminus \{0\}$ . For every  $i \in \{0, 1, \dots, k-1\}$ , let*

$$\pi_i(x) := x \left( a_i x^{p^r-1} - a_i T_{q^n|q}(x)^{p^r-1} + G(T_{q^n|q}(x)) + \alpha^{p^i} \right)$$

for some  $a_i \in \mathbb{F}_q$ . Then the function  $F = (f_0, f_1, \dots, f_{k-1}) : \mathbb{F}_{q^n}^2 \rightarrow \mathbb{F}_p^k$ , where

$$f_i(x, y) := T_{q^n|p}(x\pi_i(y) + g_i(y)),$$

is a  $(2mn, k)$ -bent function.

*Proof.* By Lemma 6.1 we need to show that every non-zero linear combination over  $\mathbb{F}_p$  of the  $\pi_i$ 's is a permutation of  $\mathbb{F}_{q^n}$ . Let  $(c_0, c_1, \dots, c_{k-1}) \in \mathbb{F}_p^k \setminus \{0\}$  and note that  $\sum_{i=0}^{k-1} c_i \alpha^{p^i} \neq 0$ . It follows that  $x(\sum_{i=0}^{k-1} c_i G(x) + \sum_{i=0}^{k-1} c_i \alpha^{p^i})$  is a permutation of  $\mathbb{F}_q$  (by our assumption on  $\bar{f}$  as well). Then

$$\sum_{i=0}^{k-1} c_i \pi_i(x) = x \left( \sum_{i=0}^{k-1} c_i a_i x^{p^r-1} - \sum_{i=0}^{k-1} c_i a_i T_{q^n|q}(x)^{p^r-1} + \sum_{i=0}^{k-1} c_i G(T_{q^n|q}(x)) + \sum_{i=0}^{k-1} c_i \alpha^{p^i} \right)$$

is a permutation of  $\mathbb{F}_{q^n}$  by Corollary 3.3 if  $\sum_{i=0}^{k-1} c_i a_i = 0$ , and by Theorem 3.4 and Corollary 3.5 otherwise.  $\square$

Theorem 6.2 generalizes Theorem 5.9 in [25].

## 7. CONCLUSION

In this paper we gave the compositional inverses of linearized binomials permuting the kernel of the trace map under the assumption that it does not permute the entire finite field in question. Previously it had been obtained in [33] the compositional inverses of linearized permutation binomials. The significance of our result lies in its applications to obtaining the compositional inverses of certain classes of permutation polynomials relying on the trace map, say the complete mapping of Theorem 3.4. The compositional inverse of this mapping was obtained in Section 4. We also gave an improvement of a class of complete mappings recently given in [34] as well as obtained a recursive construction of complete mappings involving multi-trace functions. Finally we used the improved complete mapping to construct a new class of mutually orthogonal Latin squares by means of the so called diagonal method, and to derive a  $p$ -ary bent vectorial function from the Maiorana-McFarland class.

## REFERENCES

- [1] A. Akbary and Q. Wang, *On polynomials of the form  $x^r f(x^{(q-1)/l})$* , Int. J. Math. Math. Sci. (2007), Article ID 23408, 7 pages.
- [2] A. Akbary, D. Ghioca and Q. Wang, *On constructing permutations of finite fields*, Finite Fields Appl. 17 (2011), no. 1, 51–67.
- [3] A. Akbary, D. Ghioca and Q. Wang, *On permutation polynomials with prescribed shape*, Finite Fields Appl. 15 (2009), no. 2, 195–206.

- [4] X. Cao, L. Hu and Z. Zha, *Constructing permutation polynomials from piecewise permutations*, Finite Fields Appl. 26 (2014), 162–174.
- [5] A. Çeşmelioglu, W. Meidl and A. Pott, *Generalized Maiorana-McFarland class and normality of  $p$ -ary bent functions*, Finite Fields Appl. 24 (2013), 105–117.
- [6] P. Charpin and G. Kyureghyan, *When does  $G(x) + \text{Tr}(H(x))$  permute  $\mathbb{F}_{p^n}$ ?*, Finite Fields Appl. 15 (2009), no. 5, 615–632.
- [7] R. S. Coulter and M. Henderson, *The compositional inverse of a class of permutation polynomials over a finite field*, Bull. Austral. Math. Soc. 65 (2002), 521–526.
- [8] R. S. Coulter, M. Henderson and R. Mathews, *A note on constructing permutation polynomials*, Finite Fields Appl. 15 (2009), no. 5, 553–557.
- [9] C. Ding, *Cyclic Codes from some monomials and trinomials*, SIAM J. Discrete Math. 27 (2013), no. 4, 1977–1994.
- [10] C. Ding and J. Yuan, *A family of skew Hadamard difference sets*, J. Combin. Theory Ser. A 113 (2006), 1526–1535.
- [11] N. Fernando and X. Hou, *A piecewise construction of permutation polynomial over finite fields*, Finite Fields Appl. 18 (2012), 1184–1194.
- [12] X. Hou, *Two classes of permutation polynomials over finite fields*, J. Combin. Theory Ser. A 118 (2011), no. 2, 448–454.
- [13] X. Hou, *A new approach to permutation polynomials over finite fields*, Finite Fields Appl. 18 (2012), no. 3, 492–521.
- [14] G.M. Kyureghyan, *Constructing permutations of finite fields via linear translators*, J. Combin. Theory Ser. A 118 (2011), no. 3, 1052–1061.
- [15] Y. Laigle-Chapuy, *A note on a class of quadratic permutation polynomials over  $\mathbb{F}_{2^n}$* , Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, in: Lecture Notes in Comput. Sci., vol. 4851, Springer, (2007), 130–137.
- [16] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory*, Finite Fields Appl. 13 (2007), 58–70.
- [17] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., Encyclopedia Math. Appl., vol. 20, Cambridge University Press, Cambridge, (1997).
- [18] A. Muratović-Ribić and E. Pasalic, *A note on complete polynomials over finite fields and their applications in cryptography*, Finite Fields Appl. 25 (2014), 306–315.
- [19] J. E. Marcos, *Specific permutation polynomials over finite fields*, Finite Fields Appl. 17 (2011), no. 2, 105–112.
- [20] G.L. Mullen and Q. Wang, *Permutation polynomials of one variable*, in: Handbook of Finite Fields, Chapman and Hall/CRC, (2013), Section 8.1, 215–230.
- [21] A. Muratović-Ribić, *A note on the coefficients of inverse polynomials*, Finite Fields Appl. 13 (2007), no. 4, 977–980.
- [22] R.L. Rivest, A. Shamir and L.M. Adelman, *A method for obtaining digital signatures and public-key cryptosystems*, ACM Commun. Comput. Algebra 21 (1978), 120–126.
- [23] K. Nyberg, *Perfect non-linear S-boxes*, Proc. Advances in Cryptology, EUROCRYPT (1991), LNCS, vol. 547, Springer, Heidelberg, (1992), 378–386.
- [24] A. Sade, *Groupoides automorphes par le groupe cyclique*, Canad. J. Math. vol. 9, (1957), 321–335.
- [25] S. Samardjiska and D. Gligoroski, *Quadratic permutation polynomials, complete mappings and mutually orthogonal Latin squares*, preprint.
- [26] J. Schwenk and K. Huber, *Public key encryption and digital signatures based on permutation polynomials*, Electron. Lett. 34 (1998) 759–760.
- [27] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay and S. Maitra, *Investigations on bent and negabent functions via the nega-Hadamard transform*, IEEE

- Trans. Inf. Theory 58 (6) (2012) 4064–4072.
- [28] Z. Tu, X. Zeng, L. Hu, *Several classes of complete permutation polynomials*, Finite Fields Appl. 25 (2014), 182–193.
  - [29] A. Tuxanidy, Q. Wang, *On the inverses of some classes of permutations of finite fields*, Finite Fields Appl. 28 (2014), 244–281.
  - [30] Q. Wang, *On inverse permutation polynomials*, Finite Fields Appl. 15 (2009), 207–213.
  - [31] Q. Wang, *On generalized Lucas sequences*, Combinatorics and Graphs: the twentieth anniversary conference of IPM, May 15–21, (2009), Contemporary Mathematics 531 (2010), 127–141.
  - [32] Q. Wang, *Cyclotomy and permutation polynomials of large indices*, Finite Fields Appl. 22 (2013), 57–69.
  - [33] B. Wu, *The compositional inverses of linearized permutation binomials over finite fields*, arXiv:1311.2154v1 [math.NT], preprint (2013).
  - [34] B. Wu and D. Lin, *Complete permutation polynomials induced from complete permutations of subfields*, arXiv:1312.5502v1 [math.NT], preprint (2013).
  - [35] B. Wu and D. Lin, *On constructing complete permutation polynomials over finite fields of even characteristic*, arXiv:1310.4358v2 [math.NT], preprint (2013).
  - [36] B. Wu and Z. Liu, *Linearized polynomials over finite fields revisited*, Finite Fields Appl. 22 (2013), 79–100.
  - [37] B. Wu and Z. Liu, *The compositional inverse of a class of bilinear permutation polynomials over finite fields of characteristic 2*, Finite Fields Appl. 24 (2013), 136147.
  - [38] G. Wu, N. Li, T. Helleseth and Y. Zhang, *More classes of complete permutation polynomials over  $\mathbb{F}_q$* , arXiv:1312.4716v2 [cs.IT], preprint (2013).
  - [39] P. Yuan and C. Ding, *Permutation polynomials over finite fields from a powerful lemma*, Finite Fields Appl. 17 (2011), no. 6, 560–574.
  - [40] P. Yuan and C. Ding, *Further results on permutation polynomials over finite fields*. Finite Fields Appl. 27 (2014), 88–103.
  - [41] Z. Zha and L. Hu, *Two classes of permutation polynomials over finite fields*, Finite Fields Appl. 18 (2012), no. 4, 781–790.
  - [42] M. Zieve, *Classes of permutation polynomials based on cyclotomy and an additive analogue*, in: Additive Number Theory, Springer, (2010), 355–361.

SCHOOL OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, 1125 COLONEL BY DRIVE, OTTAWA, ONTARIO, K1S 5B6, CANADA.

E-mail address: AleksandrTuxanidyTor@cmail.carleton.ca, wang@math.carleton.ca